AEGS PCI DSS

Mike Phillips

2014/07/01 14:18

Table of Contents

Contents

Show

Payment Card Industry (PCI) Data Security Standards (DSS)

The State of Iowa has a number of systems that collect electronic payments. The Information Technology Enterprise (ITE) manages the ePayment service which is a state run system that allows other state systems to collect payments. As a result of offering the ePayment service, ITE is required to be PCI DSS compliant. This document defines the policies of ITE's Applications and eGovernment Services (AEGS) division that help AEGS maintain PCI DSS compliance.

PCI DSS as it Applies to AEGS

The PCI DSS is a large body of work and its scope reaches well throughout an IT organization. However, only a portion of the twelve sections of the PCI DSS applies to the Applications and eGovernment Services division. Specifically:

- All of *Section 3 Protect Stored Cardholder Data*
- Parts of *Section 4 Encrypt transmission of cardholder data across open, public networks*
- Parts of *Section 6 Develop and maintain secure systems and applications*
  The rest of this document addresses AEGS policies regarding just the sections of the PCI DSS mentioned above.

Section 3 Protect Stored Cardholder Data

PCI DSS Section 3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

Cardholder data is not stored within ePayment. ePayment acts as proxy to an authorized payment gateway like Authorize.net so the cardholder data is passed through ePayment but none of the information including the PAN in stored in the ePayment database. Proof of this is in the ePayment database schema as well as the ePayment application log files. **NOTE: the schema linked to was produced on 8/9/2007, the most up-to-date version can be requested from the AEGS database services team.**

PCI DSS Section 3.2 Do not store sensitive authentication data subsequent to authorization even if encrypted: Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3

Please refer to PCI DSS Section 3.1 above. The primary account number (PAN), personal identification number (PIN) and card verification code are never stored by ePayment.

PCI DSS Section 3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed

Please refer to PCI DSS Section 3.1 above. The primary account number (PAN), personal identification number (PIN) and card verification code are never stored and therefore are never displayed by ePayment.

PCI DSS Section 3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches

Please refer to PCI DSS Section 3.1 above. The primary account number (PAN), personal identification number (PIN) and card verification code (CVC) are never stored and therefore are never displayed by ePayment.

PCI DSS Section 3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse

Please refer to PCI DSS Section 3.1 above. Because we don't store sensitive cardholder data such as the PAN, PIN and CVC we have no need for encryption with the exception of when passing payment requests to the payment gateway (currently Authorize.net) in which case Secure Sockets Layer (SSL) is used. For PCI DSS compliance issues related to transmission of cardholder data please refer to the ITE PCI-DSS Sharepoint Website.

PCI DSS Section 3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following

Please refer to PCI DSS Section 3.5 above. Because we don't store sensitive cardholder data we have need for encryption and there for key management is not needed.

Section 4 Encrypt transmission of cardholder data across open, public networks

See ITE PCI-DSS Sharepoint Website (or AEGS Database Services can add their stuff here).

Section 6 Develop and maintain secure systems and applications

PCI DSS 6.3.2 Separate development, test and production environments

ITE's organizational policy (link needed) is to provide separate development test and production environments. The PCI DSS standard does not mention how virtualized setups apply to this policy. That said, for PHP and other Linux-based applications we provide virtual machines for development, test and production. For windows-based systems ITE has a mixed environment of virtualized machines and physical servers. The PCI DSS does not mention if the database environment must meet his policy as well. For virtualized environment using open source database platforms like MySQL the database servers are typically running on the virtualized application servers. For proprietary database management systems like Microsft SQL Server and IBM DB2 there are single physical servers representing development, test and production. For PCI DSS compliance regarding the physical machines and the networks they run on please check the ITE PCI-DSS Sharepoint Website

PCI DSS 6.3.3 Separation of duties between development, test and production environments

AEGS Policies regarding the duties of development, test and production environment are as follows:

- Development environments are volatile with frequent code updates and database changes. This environment is for use only by developers and, when needed, the assistance of ITE Infrastructure Services. In this environment developers can push code.
- Test environments host baselines system from development that have been deemed fairly stable and ready for testing. This environment is used by the AEGS software test staff and is also used for customer verification. In this environment only ITE Infrastructure Services staff may push code.
- Production environments host baselines from test that have been deemed stable and ready for production use. This environment is only used by the customer and code and other configuration changes can only be made by ITE's Infrastructure Services after approval by the Change Advisory Board.

PCI DSS 6.3.4 Production data (live PANs) are not used for testing or development

ITE ePayment developers and ePayment customer applications test the service by using the test credit card numbers given by Authorize.net.

PCI DSS 6.3.5 Removal of test data and accounts before production systems become active

The ePayment service uses a separate database for development, test and production so there is never a concern that test data or test accounts will be migrated from one environment to another. This only applies to the ePayment and AEGS developed applications hosted at ITE.

PCI DSS 6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers

Please refer to PCI DSS 6.3.5 above. ePayment and AEGS developed applications hosted at ITE all have separate databases between the development, test and production environments.

PCI DSS 6.3.7 Review of custom code prior to release to production or customers, to identify any potential coding vulnerability

ITE's security team has implemented a process requiring all applications collecting payment through ITE's ePayment system to go through a security scan before it's production release.&nbsp; This is facilitated, in part, by the ITE code migration request.&nbsp; That form asks if the application collects electronic payments and, if so, the date of the last successful scan.&nbsp; This form notifies both ITE's operational team and the security team that a code scan is required.

Please see ITE's security team headed up by Greg Faye for more information on the tool and how it helps ensure PCI compliance during it's scan of ITE hosted applications.

PCI DSS 6.5 Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following

AEGS adheres to the Software Development Lifecycle and ITE Developer Guides. Items referenced in those document that are specifically related to PCI DSS are below. **Reminder: This section only applies to the ePayment service as well as AEGS developed applications hosted at ITE.**

PCI DSS 6.5.1 Unvalidated input

Applications that submit or process electronic payments must validate that the input given by a user is of the right data type and in the right format.

PCI DSS 6.5.2 Broken Access Control

The ePayment Service and most AEGS developed application make use of ITE's Enterprise Authentication and Authorization (A&A) Service. A&A is a centralized service that provides applications a consistent and secure way of implementing authentication and authorization within applications. A&A and any AEGS developed applications (including those that do not use A&A) are put under the further scrutiny of our software testing process as covered in the SDLC. Additionally the said systems must also undergo code reviews as described in PCI DSS 6.3.7 above.

PCI DSS 6.5.3 Broken authentication and session management (use of account credentials and session cookies)

Please refer to PCI DSS 6.5.2 above.

PCI DSS 6.5.4 Cross-site scripting (XSS) attacks

In addition to validating input as described in PCI DSS 6.5.1 above, XSS attacks can also be prevented by escaping all output. It is AEGS policy that all applications, particularly those that collect or process electronic payments, escape all output so that web browsers will not interpret potentially malicious JavaScript.

PCI DSS 6.5.5 Buffer overflow

AEGS only develops applications in PHP, Java, C#, ASP and Visual Basic. None of those languages allow for explicit memory management like C so explicit buffer overflow testing is not required. It should be noted that the consequence of this is that should buffer overflows exist in the languages themselves AEGS could be exposed to those vulnerabilities. AEGS mitigates this risk by our compliance to PCI DSS 6.1 which is covered by ITE's Infrastructure Services and is covered in detail in the ITE PCI-DSS Sharepoint Website.

PCI DSS 6.5.8 Insecure Storage

Please refer to PCI DSS 3.5 above. The ePayement Service and AEGS developed applications hosted at ITE do not store sensitive cardholder data. Furthermore it is ITE policy that all passwords (such as those used in A&A) be stored using a one-way cryptographic hash algorithm such as SHA-256 or MD5.

PCI DSS 6.5.10 Insecure Configuration Management

Configuration management includes software, hardware and operational. Regarding operational configuration management ITE's policy is to adhere to ITIL standards as closely as possible, though, no form of ITIL certification has taken place (nor is ITIL certification required by PCI DSS). Hardware configuration management is not a function of AEGS so please refer to the ITE PCI-DSS Sharepoint Website. As far as addressing software configuration management AEGS this is convered in its entirety in the AEGS Software Development Lifecycle

PCI DSS 6.6.1 Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security

The ITE Information Security Office (ISO), at their discretion, may review any code that is developed or hosted at ITE. Because the ITE ISO does not exercise this ability very often, ITE is compliant with PCI DSS 6.6.2 which requires an application layer firewall in front of all web facing application. According to PCI DSS 6.6 by fulfilling PCI 6.6.1 **or** 6.6.2 (in this case 6.6.2) we are compliant. Please refer to the ITE PCI-DSS Sharepoint Website for information on compliance with PCI DSS 6.6.2 as networking and firewall is not a function of AEGS.

Disclaimers

- this docuemnt does not address PCI DSS as it relates to ePayment customer applications. Each state agency *hosting* an application that collects electronic payments is required to be PCI DSS compliant. To be clear, this document only covers the ePayment service as well as ITE developed applications and only as it pertains to AEGS. Complete PCI DSS documentation for ITE can be found on the ITE PCI-DSS Sharepoint Website.
- Should anything in the SDLC or Developer Guides be missing or inconsistent with this document, this document's policies should be assumed.

PCI DSS Resources

- Full Text of the PCI DSS
- PCI Security Standards Council
- ITE PCI-DSS Sharepoint Website
- ePayment Documentation
- Software Development Lifecycle
- ITE Developer Guides

Possible Compliance Issues

- Do virtual machines (e.g. many virtual servers running on one physical machine) meet the PCI DSS requirement in 6.3.2 above?
- PCI DSS doesn't address whether or not the database server has to be separate from the application server. Does this have any effect on 6.3.2 above?
- The assumption with 6.3.5 and 6.3.6 is that having separate databases for development, test and production addresses this. Does it?